

JENNIFER STISA GRANICK (California Bar No. 168423)

jennifer@eff.org

MARCIA HOFMANN (California Bar No. 250087)

marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION

454 Shotwell Street

San Francisco, CA 94110

Telephone: (415) 436-9333 x134

Fax: (415) 436-9993 (fax)

Attorneys for *Amici Curiae*

Electronic Frontier Foundation, et al.

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW JERSEY

UNITED STATES,

Plaintiff,

v.

KENNETH LOWSON,
a/k/a "Money",
KRISTOFER KIRSCH,
a/k/a "Robert Woods",
JOEL STEVENSON and
FAISAL NAHDI.,

Defendants.

Criminal Case No. 10-114 (KSH)

**BRIEF OF *AMICI CURIAE*
ELECTRONIC FRONTIER
FOUNDATION, ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS OF
NEW JERSEY, ET AL. IN SUPPORT OF
DEFENDANTS' MOTION TO DISMISS
THE INDICTMENT**

Hon. Katharine S. Hayden

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	iii
STATEMENT OF INTEREST OF <i>AMICI CURIAE</i>	1
I. INTRODUCTION AND FACTS	4
A. Summary Of The Argument	4
B. The Relationship Between the Primary and Secondary Markets for Tickets	5
1. The Primary and Secondary Markets for Tickets.....	6
2. Consumer Interests Diverge from OTVs’ Interests in the Secondary Market	6
3. Ticketmaster Benefits Economically From Discouraging Broker- and Fan-Sourced Tickets in the Secondary Market	7
4. Ticketmaster Tries To Control the Secondary Market Through Paperless Tickets.....	9
5. Ticketmaster and Other OTVs Try To Control the Secondary Market Through Terms of Service	10
II. THIS COURT SHOULD DISMISS THE COMPUTER FRAUD AND ABUSE ACT CHARGES AGAINST DEFENDANTS BECAUSE THE ALLEGED VIOLATIONS OF THE OTVS TERMS OF USE DO NOT CONSTITUTE “UNAUTHORIZED ACCESS” OR “EXCEEDING AUTHORIZED ACCESS” ...	11
A. The Computer Fraud and Abuse Act Prohibits Trespass And Theft, Not Mere Contractual Violations Of Terms Of Use	13
B. The Legislative History Supports The View That The CFAA Prohibits Trespass And Theft, Not Improper Conduct by Otherwise Authorized Users.	16
III. IMPOSING CRIMINAL LIABILITY BASED ON TERMS OF SERVICE WOULD BE AN EXTRAORDINARY AND DANGEROUS EXTENSION OF CRIMINAL LAW.....	20
A. Website Policies, Including Those Of The OTVs, Contain Items That Are Likely Routinely Violated, Thus Making Potentially Millions Of Americans Into Criminals Under the Government’s Theory	20
B. Web Site Terms Are Created by Private Site Owners for a Myriad of Business Reasons Having Nothing To Do With The Public Interest or With Regulating “Access” for CFAA Purposes	23
C. Terms of Service are Often Poorly Accessible, Hard to Understand and Rarely Read.	25

IV. APPLICATION OF THE CFAA WHEN A USER IGNORES OR VIOLATES
WEBSITE TERMS OF SERVICE WOULD VIOLATE DUE PROCESS AND
RENDER THE STATUTE VOID FOR VAGUENESS.....28

VII. CONCLUSION.....31

TABLE OF AUTHORITIES**Cases**

<i>Brett Senior & Associates, P.C. v. Fitzgerald</i> , 2007 WL 2043377 (E.D. Pa. July 13, 2007)	15
<i>City of Chicago v. Morales</i> , 527 U.S. 41 (1999)	29
<i>Coates v. City of Cincinnati</i> , 402 U.S. 611 (1971)	31
<i>Diamond Power Int'l, Inc. v. Davidson</i> , 540 F. Supp. 2d 1322 (N.D. Ga. 2007)	14
<i>Douglas v. U.S. Dist. Court for Cent. Dist. Calif.</i> , 495 F.3d 1062, (9th Cir. 2007)	28
<i>Dowling v. United States</i> , 473 U.S. 207 (1985)	19
<i>Educ'al Testing Service v. Stanley H. Kaplan, Educ'al Ctr., Ltd.</i> , 965 F. Supp. 731 (D. Md. 1997)	14
<i>Foti v. City of Menlo Park</i> , 146 F.3d 629 (9th Cir. 1998)	21
<i>Grayned v. Rockford</i> , 408 U.S. 104 (1972)	29
<i>Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda</i> , 390 F. Supp. 2d 479 (D. Md. 2005)	13, 14, 16, 17
<i>International Airport Centers, LLC v. Citrin</i> , 440 F.3d 418 (7th Cir. 2006)	15
<i>Kreimer v. Bureau of Police for Town of Morristown</i> , 958 F.2d 1242 (3d Cir. 1992)	29
<i>Lockheed Martin Corp. v. Speed</i> , 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006)	15
<i>LVRC Holdings, LCC v. Brekka</i> , 581 F.3d 1127 (9th Cir. 2009)	14, 15
<i>Shamrock Foods v. Gast</i> , 535 F. Supp. 2d 962 (D. Ariz. 2008)	14
<i>Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.</i> , 119 F. Supp. 2d 1121 (W.D. Wash. 2000)	16
<i>Sony Corp. of America v. Universal City Studios, Inc.</i> , 464 U.S. 417 (1984)	19
<i>Ting v. AT & T</i> , 182 F. Supp. 2d 902, (N.D. Cal. 2002)	26
<i>United States v. Batchelder</i> , 442 U.S. 114 (1979)	29
<i>United States v. Carr</i> , 513 F.3d 1164 (9th Cir. 2008)	15
<i>United States v. Drew</i> , 259 F.R.D. 449 (C.D. Cal. 2009)	1, 24
<i>United States v. LaMacchia</i> , 871 F. Supp. 535 (D. Mass. 1994)	18, 19

<i>United States v. Nosal</i> , 2010 WL 934257 (N.D. Cal. Jan. 6, 2010).....	15
<i>United States v. Riggs</i> , 739 F.Supp. 414 (N.D. Ill. 1990)	18
<i>Zadvydas v. Davis</i> , 533 U.S. 678 (2001).....	31

Statutes

18 PA. CONS. STAT. § 6910 (1973)	19
18 U.S.C. § 1030.....	passim
18 U.S.C. § 2701.....	13
720 ILL. COMP. STAT. 375/1.5 (2005)	19
ALA. CODE § 40-12-167 (1975).....	19
ARK. CODE ANN. § 5-63-201 (2005).....	19
CAL. PENAL CODE § 346 (1972).....	19
FLA. STAT. § 817.36 (2010).....	19
GA. CODE ANN. § 43-4B-31 (2001)	19
GA. CODE ANN. § 43-4B-25	19
HAW. REV. STAT. § 440-17 (1983)	19
KY. REV. STAT. ANN. § 518. 070 (1974).....	19
MASS. GEN. LAWS CH. 140, § 185G (1980).....	19
MASS. GEN. LAWS CH. 140, §185A (1980).....	19
MD CODE, BUSINESS REGULATION, § 4-318 (1992).....	19
MICH. COMP. LAWS § 750. 465 (2005)	19
N. J. REV. STAT. § 56: 8-26 (2008).....	19
N. J. REV. STAT. § 56: 8-38 (2008).....	19
N.C. GEN. STAT. § 14-344 (2008).....	19
N.Y. ARTS & CULT. AFF. § 25.01	19
N.Y. ARTS & CULT. AFF. § 25.35 (1983).....	19
R. I. GEN LAWS § 5-22-26 (1988).....	19
S.C. CODE ANN. 16-17-710 (2006).....	19

S.D. CODIFIED LAWS § 9-34-8 (1992).....	19
VA. CODE ANN. § 15.2-969 (2009).....	19
WIS. STAT. § 42.07 (1990).....	19

Other Authorities

Alan M. White & Cathy Lesser Mansfield, <i>Literacy and Contract</i> , 13 Stan. L. Rev. 233 (2002)	27
Mark A. Lemley, <i>Terms of Use</i> , 91 Minn. L. Rev. 459 (2006).....	22
Melvin Aron Eisenberg, <i>The Limits of Cognition and the Limits of Contract</i> , 47 Stan. L. Rev. 211 (1995).....	27
Michael I. Meyerson, <i>The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts</i> , 47 U. Miami L. Rev. 1263 (1993)	26, 27
Orin S. Kerr, <i>Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes</i> , 78 N.Y.U. L. Rev. 1596 (2003).....	30
Orin S. Kerr, <i>Vagueness Challenges to the Computer Fraud and Abuse Act</i> , Minn. L. Rev. (forthcoming 2010)	21, 30
Restatement (Second) of Agency §112 (1958).....	16
Restatement (Second) of Contracts § 211 (1981).....	26
Robert A. Hillman & Jeffrey J. Rachlinski, <i>Standard-Form Contracting in the Electronic Age</i> , 77 N.Y.U. L. Rev. 429 (2002)	26
Robert L. Oakley, <i>Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts</i> , 42 Hous. L. Rev. 1041 (2005).....	26
Robert W. Gomulkiewicz, <i>Getting Serious About User-Friendly Mass Market Licensing for Software</i> , 12 Geo. Mason L. Rev. 687 (2004).....	27
Russell Korobkin, <i>Bounded Rationality, Standard Form Contracts, and Unconscionability</i> , 70 U. Chi. L. Rev. 1203 (2003)	27

Legislative Authorities

141 Cong. Rec. S 9423 (daily ed. June 29, 1995).....	17
142 Cong. Rec. E1621 (daily ed. Sept. 17, 1996).....	17
Better Oversight of Secondary Sales and Accountability in Concert Ticketing Act (BOSS ACT), H.R. 2669, 111th Cong. (2009).....	19
H.R. Rep. No. 98-894 (1984), reprinted in 1984 U.S.C.C.A.N. 3689.....	17
Pub. L. No. 98-473, § 2102(a), 98 Stat. 1937 (1984).....	16

S. Rep. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479..... 16, 17

STATEMENT OF INTEREST OF AMICI CURIAE

Amici's interest in this case is the sound and principled interpretation and application of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. *Amici* believe that this brief may assist the Court in its consideration of how consumer interests could be affected by the outcome of this case, as well as the proper scope of section 1030 in general.

Electronic Frontier Foundation ("EFF") is a non-profit, member-supported digital civil liberties organization. As part of its mission, EFF has served as counsel or *amicus* in key cases addressing user rights to free speech, privacy, and innovation as applied to the Internet and other new technologies. With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org. EFF has filed *amicus* briefs or represented parties in several cases involving terms of service and claims of criminal law violations including *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) ; *In Re Matter Of Search Warrant Executed On March 30, 2009 At The Residence Of Movant Riccardo Calixte*, Massachusetts Supreme Judicial Court For Suffolk County, No. SJ-2009-0212 (court opinion available at <http://www.eff.org/files/filenode/inresearchBC/SJCcalixteorder.pdf>); and *Facebook Inc. v. Power Ventures*, Northern District of California, Case No. 5:08-cv-05780 (brief available at http://www.eff.org/files/filenode/facebook_v_power/FBvPower_June%20Amicus%20Final.pdf).

The Association of Criminal Defense Lawyers of New Jersey is comprised of approximately 450 members of the criminal defense bar of this State. Members include

attorneys in private practice and public defenders. The ACDL-NJ has participated in numerous cases in the courts of the United States and the courts of the State of New Jersey. On various occasions, the ACDL-NJ affirmatively has been requested by this Court to file *amicus* briefs on matters of importance to the Court. In addition, ACDL-NJ has been requested by this Court to articulate positions on ethical matters and on proposed changes in rules and policies relating to the criminal justice system. Numerous cases in which the ACDL-NJ has appeared as *amicus* have resulted in significant decisions.

The Center for Democracy and Technology is a non-profit public interest organization working to keep the Internet open, innovative, and free. As a civil liberties group with expertise in law, technology, and policy, CDT works to enhance free expression and privacy in communications technologies by finding practical and innovative solutions to public policy challenges while protecting civil liberties. In particular, CDT has worked to protect the right of Internet users to visit public web sites without fear of criminal charges based on provisions within the site's terms of service.

Law professor *amici* are:

- Gabriel "Jack" Chin, Chester H. Smith Professor of Law, Professor of Public Administration and Policy and Director, Program in Criminal Law and Policy, University of Arizona, James E. Rogers College of Law
- Eric Goldman, Director, High Tech Law Institute, Santa Clara University School of Law
- Michael Risch, Associate Professor of Law, Villanova University School of Law
- Ted Sampsell-Jones, Assistant Professor of Law, William Mitchell College of Law
- Robert Weisberg, Edwin E. Huddleson, Jr. Professor of Law, Director of the

Stanford Criminal Justice Center, Stanford Law School

These *amici* are individual faculty members who research, teach and write scholarly articles and books about Internet law, cybercrime, criminal law and related topics at law schools nationwide. None received any compensation for participating in this brief. Law professor *amici*'s sole interest in this case is in the evolution of sound and principled interpretation and application of the Computer Fraud and Abuse Act.

I. INTRODUCTION AND FACTS

The government seeks criminal convictions against several men in the business of purchasing tickets for resale from Online Ticket Vendors (“OTV”s). It is not a crime to purchase tickets with the intent to resell them, or to resell tickets on the secondary market. Despite this fact, this prosecution would give OTVs immense control over the downstream sale of tickets purchased from their sites, through their website terms of use. On the government’s view, when someone disregards a condition in terms of use, their access to the website is no longer authorized and that unauthorized access violates the Computer Fraud and Abuse Act. *Amici* reject this expansion of the criminal law because it is contrary to the statute, Constitution and sound public policy. This Court should grant Defendants’ motion to dismiss the indictment.

A. Summary Of The Argument

Though the actions underlying the criminal charges in this matter took place in “cyberspace”, this case is very much about real-world stadiums, theaters and concert halls, and who may profit from the sale of tickets to events held there. When performances are popular, fans are often willing to pay more than face value for tickets to those shows. Resale is a robust and profitable business, estimated to soon be worth almost \$4.5B per year.¹ The rapid growth of the ticket resale business indicates that many consumers like the convenience of buying tickets closer to the date of performances, even at a higher price.

Yet the entertainment industry – and the OTVs that comprise the alleged victims in this case – do not like ticket resale. They view downstream sales as profits that should rightfully go to performers, producers or OTVs, but have been lost to the secondary market. Primary ticket sources try to discourage resale of the tickets they sell. They do so

¹ Sucharita Mulpuru & Peter Hult, *Forrester, The Future of Online Secondary Ticketing*, 5 (2008) (“We predict that online secondary ticketing will continue to experience near-double-digit growth, with online event ticket sales expected to reach a healthy \$4.5 billion in 2012 — a 12% compound annual growth rate.”).

by posting website terms of use that prohibit a variety of resale-related activities, including automated purchase, bulk purchase and purchase with the intent to resell. *Amici* do not argue that OTVs may not impose contractual terms on customers. However, this prosecution backs up OTVs' business preferences with the force of criminal law,² interfering with fairness, social welfare and due process.

The government's basic allegation is that Defendants purchased tickets from the OTVs in violation of the OTVs' terms of service prohibiting automated access. It would be extremely dangerous, however, for this Court to determine that mere violations of terms of service violate criminal law. To hold otherwise, as the government urges this Court to do, will expand the scope of the CFAA beyond what Congress intended. It will (1) give private parties immense latitude to decide what conduct is criminal, (2) create legal uncertainty for users and the risk of capricious enforcement by government and (3) ground criminal liability in the arbitrary and often confusing terms that websites wish to impose on users. Given the range of activity that is currently subject to online terms of use, millions of otherwise innocent Internet users will violate criminal law every day through routine online behavior. For these reasons, *amici* urge the Court to dismiss the indictment.

B. The Relationship Between the Primary and Secondary Markets for Tickets

The government suggests that this case is about ensuring the public's fair access to event tickets, and that Defendants harmed fans by jumping to the front of the virtual line for ticket purchase. Whatever the impropriety of cutting the line for goods offered to the general public, doing so is not a CFAA offense. Moreover, this Court should not presume that fans benefit from Ticketmaster and other OTVs' control over the market. A closer look at Ticketmaster and other OTVs' business interests reveals the public interest

² Denying criminal liability here will not leave OTVs without a remedy. Assuming the their terms of use are enforceable, the OTVs have civil and contractual remedies available to them, including seeking appropriate damages.

may well be served by a robust secondary marketplace and that imposing criminal liability in this case is counter to that public interest.

1. The Primary and Secondary Markets for Tickets

A sports team, performing artist, event venue or promoter is commonly the primary source of tickets to a particular event. The primary source sets ticket prices (also known as the face value) and distributes the tickets, often through an OTV such as Ticketmaster or the companies identified as alleged victims in this case. The distribution agreements typically involve promises of exclusivity and the right to define the terms of sale. Superseding Indictment ¶¶ 2c, 2e. The distributor tacks on convenience, service and delivery fees, which can comprise a substantial portion of the purchase price.

OTVs and other primary sellers often offer tickets at prices lower than the market would bear. There are many possible reasons for this, including ensuring a sell-out or the desire to widen the fan base by making the event accessible to less economically privileged people. Paul Krugman, *Thinking Outside the Box Office: Ticket Scalping and the Future of Capitalism*, Slate (May 13, 1999) <http://slate.msn.com/id/28017/>, see also Superseding Indictment 2e. Whatever the reasons, there often are a limited number of tickets available for purchase at below-market rates. This inevitably leads to a secondary market for ticket resale. Superseding Indictment 2e.

2. Consumer Interests Diverge from OTVs' Interests in the Secondary Market

Before the Internet, if a fan could not get a ticket from a primary vendor, an individual scalper was virtually the only alternative.³ Today, tickets are readily available on Internet retail sites such as StubHub.com, the market leader in secondary ticket sales.⁴

³ Joe Milicia, *Ticketmaster's Near Monopoly Challenged As Technology Changes*, USA Today, Jan. 19, 2008, available at http://www.usatoday.com/sports/2008-01-18-48774553_x.htm ("In the 1990s, when Garth Brooks and Michael Jordan filled arenas, the only way to see them live was to go through Ticketmaster, or a scalper.").

⁴ *Top Secondary Ticket Sellers*, TicketNews, <http://www.ticketnews.com/view/TopSecondarySellers> (last visited June 30, 2010).

Consumers generally prefer to deal with companies over individuals, because the companies can offer advance purchase, money-back and other valuable guarantees,⁵ unavailable from an unknown individual standing outside a stadium. Thus, the success of the secondary market comes as no surprise. The social benefits include giving fans a market for reselling tickets they cannot use and creating more avenues and choices for ticket purchases.⁶

Yet the growth of the resale market threatens OTVs' – and particularly Ticketmaster's – hegemony over ticket sales.⁷ OTVs have made several maneuvers to try to stop people from reselling tickets outside of the OTVs' control, as described in sections 3-5 below.

3. Ticketmaster Benefits Economically From Discouraging Broker- and Fan-Sourced Tickets in the Secondary Market

Ticketmaster has several business ventures designed to control the secondary market for tickets. First, Ticketmaster set up TicketExchange for sports season ticket holders to sell or trade their tickets.⁸ Second, in January 2008, Ticketmaster purchased secondary reseller TicketsNow.⁹ Finally, Ticketmaster recently merged with its competitor LiveNation, a deal that was only recently recommended for approval by the U.S. Department of Justice Antitrust Division.¹⁰ Therefore, Ticketmaster has vertical

⁵ StubHub Guarantee, <http://www.stubhub.com/guarantee/> (last visited June 30, 2010) (“We Guarantee: You will get your tickets in time for the event. Your tickets will be authentic and valid for entry. You will receive tickets comparable to or better than the tickets you ordered, or your money back. You will be refunded if the event is cancelled and is not rescheduled.”)

⁶ See, e.g., Stephen K. Happel & Marianne M. Jennings, *The Folly of Anti-scalping Laws*, Cato J., Spring/Summer 1995, at 65, available at <http://www.cato.org/pubs/journal/cj15n1-4.html>.

⁷ Milicia, *Ticketmaster's Near Monopoly Challenged*, *supra*, at 3 (“You have to look at the secondary market as something that is a real threat to Ticketmaster . . . They missed the boat. StubHub has been around a few years now already. They weren't as proactive as they probably should have been.”)

⁸ Ticketmaster TicketExchange, <http://www.ticketmaster.com/ticketexchange> (last visited June 30, 2010).

⁹ Alfred Branch, Jr., Ticketmaster/TicketsNow: After the Deal (Jan. 15, 2008), <http://www.ticketnews.com/Ticketmaster-TicketsNow-After-the-Deal018158>.

¹⁰ Alfred Branch, Jr., *DOJ Recommends Ticketmaster/Live Nation Merger*

integration and valuable relationships with venues, promoters and performers.

Ticketmaster's secondary ticket outlets seek to leverage the exclusive arrangements and relationships the company has with primary ticket sources. For example, rather than get tickets from brokers or fans as StubHub does,¹¹ TicketsNow gets tickets from the primary sources. Most, if not all, of the tickets on TicketsNow are sold through deals with primary sources Ticketmaster has cultivated relationships with in the primary market.¹²

Regulators have been concerned that the relationship between Ticketmaster and TicketsNow, not to mention other Ticketmaster practices, interferes with the interests of fans.¹³ For example, in August 2008, TicketsNow announced premium-priced Neil Diamond tickets less than a minute after regularly priced tickets went on sale. The singer was the source of the tickets, through a deal reached between his management and Ticketmaster.¹⁴ In February 2009, fans who tried to buy tickets for New York and New Jersey Bruce Springsteen concerts through Ticketmaster's website were told that the shows had sold out in minutes, and then steered to TicketsNow's website, where prices

Receive Final Approval, TicketNews (June 22, 2010), <http://www.ticketnews.com/DOJ-recommends-Ticketmaster-Live-Nation-merger-receive-final-approval6102268>.

¹¹ StubHub Help, <http://www.stubhub.com/help/> (last visited June 30, 2010) (Sellers include "season ticket holders who cannot attend every game, licensed ticket brokers, ticket holders who have changed their plans, ticket holders who are unable to attend an event," and "ticket holders with extra tickets to sell." "Sellers may be individuals, businesses, ticket brokers, corporate sponsors, promoters, fan club members, contest winners, or just about anyone who wishes to see their tickets end up in the hands of another fan.").

¹² Ethan Smith, *Concert Tickets Get Set Aside, Marked Up by Artists, Managers*, Wall. St. J., March 11, 2009, available at <http://online.wsj.com/article/SB123672740386088613.html> ("Joseph Freeman, Ticketmaster's senior vice president for legal affairs, says that the company's 'Marketplace' pages only rarely list tickets offered by fans. The vast majority of tickets are sold by the artists and their promoters with the cooperation of Ticketmaster.").

¹³ Kerry Grace Benn, *Ticketmaster Unit to Pay \$50,000 Over Deceptive Practices*, Wall. St. J., July 1, 2009, at B1, available at <http://online.wsj.com/article/SB124637740774473993.html>.

¹⁴ Smith, *supra* note 12 ("In the case of the Neil Diamond concerts, however, the source of the higher-priced tickets was the singer, working with Ticketmaster Entertainment Inc., which owns TicketExchange, and concert promoter AEG Live.")

were hundreds of dollars above face value.¹⁵ These incidents prompted calls from U.S. Representative Bill Pascrell Jr. (D-NJ) for an investigation, as well as proposed federal legislation.¹⁶ Ticketmaster denies that it holds back tickets to put on TicketsNow.¹⁷

These examples indicate that Ticketmaster may compete in the secondary market by capitalizing on its power in the primary market. The company has a competitive advantage when there is a shortage of the broker- or fan-sourced tickets that comprise the bulk of its competitors' inventory. TicketsNow can still thrive in such a dry economy, since no one has better connections for entertainment industry-sourced tickets than Ticketmaster.

4. Ticketmaster Tries To Control the Secondary Market Through Paperless Tickets

In the past two or three years, the entertainment industry and OTVs have innovated another method for controlling the downstream market for tickets: paperless ticketing. For a paperless ticket event, a consumer buys tickets with a credit card online or by telephone, goes to the venue on the day of the event with the credit card and a form of identification, and receives a seat locator at the venue by presenting her ID and swiping her credit card.¹⁸ The problem for consumers is that these paperless tickets cannot be transferred either as a gift or through resale unless both the consumer and the recipient are physically present at the venue on the day of the event.¹⁹ People who cannot

¹⁵ Adam Satariano & Greg Bensinger, *Springsteen Sellout Leads to Calls for Probe of Ticketmaster*, Bloomberg (Feb. 4, 2009), <http://www.bloomberg.com/apps/news?pid=newsarchive&refer=muse&sid=ayD73kINfON4>.

¹⁶ Alfred Branch, Jr., *House Rep. Pascrell to Introduce New Ticketing Legislation* (June 1, 2009), <http://www.ticketnews.com/House-Rep-Pascrell-to-introduce-new-ticketing-legislation6091234>.

¹⁷ Ticketmaster & TicketsNow – Questions and Answers, <http://www.ticketmaster.com/ticketsnow> (last visited July 1, 2010).

¹⁸ Ticketmaster Paperless Ticketing, <http://www.ticketmaster.com/paperless> (last visited June 30, 2010).

¹⁹ *Id.* (“Can I buy the tickets but not go to the show? Yes, if you buy tickets for friends or family, often you just have to go to the gate, not *through* the gate. Simply accompany them to the venue and show your credit card and ID to get them in!”).

attend the event for whatever reason are stuck with tickets they cannot easily transfer, and the secondary market for tickets to paperless ticket events is essentially non-existent. Legislators have considered requiring vendors to either allow consumers to choose a paper ticket or to make paperless tickets capable of being transferred after the initial sale independently from the primary source, vendor or their agents.²⁰

5. Ticketmaster and Other OTVs Try To Control the Secondary Market Through Terms of Service

Ticketmaster and other OTVs seek to prevent resale of tickets through website terms of use that purport to limit the number of tickets any one individual may buy, to prohibit automation, and sometimes even to prohibit access to the website with intent to resell. For example, Tickets.com's Terms of Use assert, "If you are seeking to purchase tickets to any event offered through this website for the purposes of reselling those tickets, then you are not authorized to enter this website and use its services." Tickets.com User Agreement, http://www.tickets.com/aboutus/user_agreement.html (last visited June 30, 2010). Similarly, Telecharge.com purports to outlaw ticket resale for any purpose through its terms of service: "You may not copy, modify, distribute, display, perform, create derivative works from, transfer or sell any information, software, products or services obtained from this web site." Telecharge Terms and Conditions, <http://www.telecharge.com/policies.aspx> (last visited June 30, 2010). These terms may benefit Tickets.com or Telecharge, but they do not benefit consumers, who may need to resell tickets when their plans change or for other reasons, or who may wish to purchase through the secondary market. Indeed, many economists agree that consumers suffer when the resale market is unduly constrained.²¹

²⁰ Alfred Branch, Jr., *New York State Senators Hear Pros and Cons of Paperless Tickets* (June 2, 2010), <http://www.ticketnews.com/New-York-State-Senators-hear-pros-and-cons-of-paperless-tickets61026715>.

²¹ See Kevin A. Hassett, *Estimating the Consumer Benefits of Online Trading* (2008) ("Scalpers' may play a useful role acting as intermediaries between event producers and consumers with uncertain demand, and may end up increasing overall welfare, rather than reducing it.").

In sum, giving OTVs more control over ticket sale and resale will not necessarily promote social welfare, and should be handled carefully and with subtlety. As Congress and state legislatures have realized in their decision not to regulate the ticket industry, the ticket business is complicated and the “right answer” is not clear. What is clear is that some people believe that consumers suffer from being stuck with non-transferrable paper tickets, from unregulated mergers, from collusion between the primary vendors and secondary vendors and from interference with the secondary market. That is why New York and other states are considering regulation of paperless ticketing. That is why the Department of Justice only approved the merger of Ticketmaster and LiveNation after requiring divestiture of some aspects of Ticketmaster’s business. That is why Congress has investigated the Bruce Springsteen incident and Ticketmaster has unlinked the primary sale venue from TicketsNow. That is why most states and the federal government have not regulated the purchase or sale of tickets in the secondary market.

None of these complexities has been given any consideration in this prosecution. Rather, the government’s view is that if Ticketmaster and other OTVs say in their terms of service that they do not want automated purchase or resale, and individuals do it anyway, then it’s a crime. This view chills otherwise lawful conduct and puts the power of criminal law behind private business interests rather than the public welfare. It should be rejected.

II. THIS COURT SHOULD DISMISS THE COMPUTER FRAUD AND ABUSE ACT CHARGES AGAINST DEFENDANTS BECAUSE THE ALLEGED VIOLATIONS OF THE OTVS TERMS OF USE DO NOT CONSTITUTE “UNAUTHORIZED ACCESS” OR “EXCEEDING AUTHORIZED ACCESS”

The fundamental question in this case is whether otherwise authorized access to a public-facing e-commerce website becomes “without authorization” or exceeds authorized access under the CFAA when the terms of use are violated. The plain language of the CFAA criminalizes a trespasser’s access to computer systems, areas of

computer networks or private data without permission. In other words, the statute prohibits trespass and theft. Notably, the statute does not criminalize improper motives for access or improper use after authorized access. The OTV websites here were open for business, to any person on the planet. The fact that some of those people chose to use automated means in violation of the websites' terms of service may result in a breach of contract claim, but does not convert otherwise authorized access into a crime.

Liability turns on the question of whether Defendants were authorized to access or exceeded authorized access of the OTVs' websites. Because the websites were open for business to the public at large, Defendants were authorized to access the websites. Although Congress did not define the phrase "without authorization," it did define the phrase "exceeds authorized access." The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The Superseding Indictment does not allege whether Defendants' access to the OTVs services was "without authorization," "in excess of authorized access," or both. The first covers outsiders who have no rights to the computer system, and the second covers "insiders" who have some rights to access the computer system, but do not have rights to access or alter certain files or information on that same system. Defendants do not fall within either category. The OTV websites were open to members of the public with no security measures to prohibit access, such as passwords. The technological measures employed were for the purpose of dissuading people from using automated means to access the site. But any person is authorized to browse the sites and access information stored there. Doing so by automated means does not convert otherwise authorized use into a crime, especially where the method did not cause any physical interference or harm to the server. Because the CFAA prohibits trespass, but not an

authorized user's bad motive or use of tools that do not cause damage to the server, Defendants committed no crime.

A. The Computer Fraud and Abuse Act Prohibits Trespass And Theft, Not Mere Contractual Violations Of Terms Of Use

The most recent cases interpreting the CFAA have held that if a user is authorized to access a computer and information stored there, doing so is not criminal, even if that access is in violation of a contractual agreement or non-negotiated terms of use. For example, in *International Association of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005), the plaintiff argued that the defendant, a union officer, exceeded her authorization to use the union computer when she violated the terms of use to access a membership list with the purpose to send it to a rival union, and not for legitimate union business. *Id.* at 495-96. The defendant had signed an agreement promising that she would not access union computers "contrary to the policies and procedures of the [union] Constitution." *Id.* The court rejected the application of section 1030, holding that even if the defendant breached a contract, that breach of a promise not to use information stored on union computers in a particular way did not mean her access to that information was unauthorized or criminal:

Thus, to the extent that Werner-Masuda may have breached the Registration Agreement by using the information obtained for purposes contrary to the policies established by the [union] Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the [Stored Communications Act] or the CFAA. . . . Although Plaintiff may characterize it as so, the gravamen of its complaint is not so much that Werner-Masuda improperly accessed the information contained in VLodge, but rather what she did with the information once she obtained it. . . . Nor do [the] terms [of the Stored Communications Act and the CFAA] proscribe authorized access for unauthorized or illegitimate purposes.

Id. at 499 (citations omitted).²²

²² The *Werner-Masuda* court similarly interpreted the same language in the Stored Communications Act, 18 U.S.C. § 2701(a) ("SCA"). It found that the SCA "prohibit[s] only unauthorized access and not the misappropriation or disclosure of information." It continued: "there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access."

Subsequent cases have followed the reasoning of *Werner-Masuda* based on either plain language or legislative history. In *Diamond Power International, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007), the court similarly rejected a CFAA claim against an employee who violated an employment agreement by using his access to his employer's computer system to steal data for a competitor. The defendant had transferred information from password-protected computer drives to his new employer while still employed with the former company, in violation of a confidentiality agreement. *Id.* at 1327-31. Identifying a narrow interpretation of "exceeding authorized access" as "the more reasoned view," the court held that "a violation for accessing 'without authorization' occurs only where initial access is not permitted. Further, a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted." *Id.* at 1343.

In *Shamrock Foods v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008), the court relied on *Davidson* and *Werner-Masuda* to hold that the defendant did not access the information at issue "without authorization" or in a manner that "exceed[ed] authorized access." *Id.* at 968. The defendant had an employee account on the computer he used at his employer, Shamrock, and was permitted to view the specific files he allegedly emailed to himself. The CFAA did not apply, even though the emailing was for the improper purpose of benefiting himself and a rival company in violation of the defendant's Confidentiality Agreement.

In *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the defendant was a marketing contractor for a residential treatment center for addicts. During negotiations to take an ownership interest in the facility, Brekka emailed several of the

Werner-Masuda, 390 F. Supp. 2d at 496 (quoting *Educ. Testing Service v. Stanley H. Kaplan Educ. Ctr., Ltd.*, 965 F. Supp. 731, 740 (D. Md. 1997) ("[I]t appears evident that the sort of trespasses to which the [SCA] applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way").

facilities' files to himself. *Id.* at 1130. Subsequently, after the talks had terminated unsuccessfully and he was no longer working for the facility, Brekka used his login information to access the center's website statistics system. *Id.* The company discovered his access, disabled the account and sued Brekka, alleging that he violated 18 U.S.C. §§ 1030(a)(2) and (a)(4) by emailing files to himself for competitive purposes and for accessing the statistics website. *Id.* The Ninth Circuit upheld summary judgment in favor of Brekka. "For purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations." *Id.* at 1133. In other words, "[a] person uses a computer 'without authorization' under [section 1030(a)(4) only] when the person has not received the permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id.* at 1135.

The plaintiff in *Brekka* had pointed to the Seventh Circuit case of *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), arguing that an employee can lose authorization to use a company computer when the employee resolves to act contrary to the employer's interest. The Ninth Circuit explicitly rejected that interpretation because section 1030 is first and foremost a criminal statute that must have limited reach and clear parameters under the rule of lenity and to comply with the void for vagueness doctrine. *United States v. Carr*, 513 F.3d 1164, 1168 (9th Cir. 2008), *noted in Brekka*, 581 F.3d at 1134.²³

The cases discussed above contrast with and reject earlier decisions, most

²³ For additional cases rejecting criminal liability under the CFAA when the defendant had authorization to access the system or data in question, but misused that authority, see also *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006); *Brett Senior & Associates, P.C. v. Fitzgerald*, 2007 WL 2043377 (E.D. Pa. July 13, 2007); *United States v. Nosal*, 2010 WL 934257 (N.D. Cal. Jan. 6, 2010).

importantly *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), often cited in support of claims that terms of service violations are criminal conduct under the CFAA. In *Shurgard*, the district court denied a motion to dismiss a CFAA claim brought by an employee who took employer information from the computer system with him to his next job. *Id.* at 1129. The court relied on the Restatement (Second) of Agency § 112 (1958) to hold that when the plaintiff's former employees accepted new jobs with the defendant, the employees "lost their authorization and were 'without authorization' [under the CFAA] when they allegedly obtained and sent [the plaintiff's] proprietary information to the defendant via e-mail." *Shurgard*, 119 F. Supp. 2d at 1125. The *Shurgard* approach has troubling and potentially unconstitutional results, most notably criminalizing employee disloyalty or other transgressions against the mere preferences of a private party.

In sum, the better-reasoned and more recent cases explicitly reject the notion that terms of service violations could create federal criminal liability.

B. The Legislative History Supports The View That The CFAA Prohibits Trespass And Theft, Not Improper Conduct by Otherwise Authorized Users.

The legislative history confirms that Congress intended the CFAA to criminalize intruders who trespassed on computers and computer networks. *Werner-Masuda*, 390 F. Supp. 2d at 495-96 (citing S. Rep. No. 99-432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482 (explaining that the CFAA "is a consensus bill aimed at deterring and punishing certain 'high-tech' crimes")). The CFAA was originally called the Counterfeit Access Device and Computer Fraud and Abuse Act and was enacted in 1984. Pub. L. No. 98-473, § 2102(a), 98 Stat. 1937 (1984). The 1984 House Committee emphasized that "section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer . . . in committing the

offense.” H.R. Rep. No. 98-894, at 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706. Consequently, the committee report emphasized concerns about “hackers” who “trespass into” computers and the inability of “password codes” to protect against this threat. H.R. Rep. No. 98-894, at 10-11, *reprinted in* 1984 U.S.C.C.A.N. at 3695-97. The 1984 version of the law criminalized actions of one who gains “unauthorized access” or who “having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.”

In 1986, Congress deleted the part of the statute that prohibited those with authorization from using the system for unauthorized purposes and substituted the phrase “exceeds authorized access.” *See Werner-Masuda*, 390 F. Supp. 2d at 499 n. 12 (quoting S. Rep. No. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486). As the court in *Werner-Masuda* explained:

By enacting this amendment, and providing an express definition for “exceeds authorized access,” the intent was to “eliminate coverage for authorized access that aims at ‘purposes to which such authorization does not extend,’” thereby “removing from the sweep of the statute one of the murkier grounds of liability, under which a [person’s] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.

Id. at 499 n. 12 (quoting S. Rep. No. 99-432, at 21, *reprinted in* 1986 U.S.C.C.A.N. at 2494-95) (alterations in original). Congress used the “exceeds authorized access” language to avoid extending criminal liability to employees where administrative sanctions were more appropriate. *Id.*

The fact that trespass rather than motive- or means based regulation was Congress’ intent is further supported by the fact that, when discussing the CFAA, and specifically section 1030(a)(2)(C), legislators often referred to “hackers” and the need to protect sensitive information from theft. *See, e.g.*, 142 Cong. Rec. E1621 (daily ed. Sept. 17, 1996) (statement of Rep. Goodlatte); *see also* 141 Cong. Rec. S 9423 (daily ed. June 29, 1995) (statement of Sen. Leahy). The modern, conventional usage of “hacker” is

usually someone who gains unauthorized access to a computer typically to obtain information of value he or she is not entitled to obtain, or to cause damage. *See, e.g.*, Oxford English Dictionary, Oxford University Press (defining, *inter alia*, a hacker as “a person who uses his skill with computers to try to gain unauthorized access to computer files or networks”); *see also United States v. Riggs*, 739 F.Supp. 414, 423-24 (N.D. Ill. 1990) (citing approvingly to sources that define hackers as those using computer skills to gain unauthorized access to a computer system). The legislative history makes no mention of unauthorized or excessive access obtained through ignorance or disregard of private terms of service.

The legislative history supports the conclusion that the CFAA criminalizes trespasses in which the user gains access to computer services or information to which he is not entitled, not those in which an authorized individual uses the services or information in an impermissible manner, or accesses those services with unapproved tools, so long as those means cause no harm to the server.

Defendants here purchased tickets at full price from a free, interactive, Internet-based e-commerce site open to anyone on the planet. OTVs perform no vetting, require no accounts, and implement no checks on who may use the service. Everyone is authorized to access the service. OTVs do seek to impose additional restrictions, but these restrictions are not properly the subject of criminal enforcement, especially where the defendant’s actions are otherwise not criminal.

In this way, this case is reminiscent of the failed prosecution in *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994), where the district court rejected a government attempt to stretch the scope of the federal wire fraud statute to cover the unauthorized, non-commercial distribution of copyrighted software products over the Internet by an MIT student. At the time, copyright law did not contain criminal provisions against non-commercial infringement. The court recognized that “[w]hat the

Government is seeking to do is to punish conduct that reasonable people might agree deserves the sanctions of the criminal law,” but that the wiser course was to leave it to Congress to prescribe crime and establish penalties. *Id.* at 544 (citing *Dowling v. United States*, 473 U.S. 207 (1985)). The court further stated:

The judiciary’s reluctance to expand the protections afforded by the copyright without explicit legislative guidance is a recurring theme. Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the institutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.

Id. (citing *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 431 (1984)).

Here, too, the government tries to use broad statutes and the vagaries of modern technology to criminalize that which Congress and the state of New Jersey have both chosen to allow. Congress could outright prohibit bulk purchase or scalping of tickets. States either fail to regulate or only lightly regulate ticket resale.²⁴ Congress has considered, but failed to enact, even these modest restrictions. (*See, e.g.*, Press Release, Senator Charles E. Schumer, Schumer Unveils New Legislation to Crack Down on Ticket Resellers and Dramatically Bring Down Prices for Fans (Apr. 6, 2009), *available at* http://schumer.senate.gov/new_website/record.cfm?id=311230; Better Oversight of Secondary Sales and Accountability in Concert Ticketing Act (BOSS ACT), H.R. 2669, 111th Cong. (2009)). What the government asks this Court to do is to read the CFAA

²⁴ *See e.g.*, ALA. CODE § 40-12-167 (1975); ARK. CODE ANN. § 5-63-201 (2005); CAL. PENAL CODE § 346 (1972); FLA. STAT. § 817.36 (2010); GA. CODE ANN. §§ 43-4B-25 to 43-4B-31 (2001); HAW. REV. STAT. § 440-17 (1983); 720 ILL. COMP. STAT. 375/1.5 (2005); KY. REV. STAT. ANN. § 518.070 (1974); MD CODE, BUSINESS REGULATION, § 4-318 (1992); MASS. GEN. LAWS CH. 140, §§185A to 185G (1980); MICH. COMP. LAWS § 750.465 (2005); N. J. REV. STAT. §§ 56:8-26 TO 56:8-38 (2008); N.Y. ARTS & CULT. AFF. §§ 25.01 to 25.35 (1983); N.C. GEN. STAT. § 14-344 (2008); 18 PA. CONS. STAT. § 6910 (1973); R. I. GEN LAWS § 5-22-26 (1988); S.D. CODIFIED LAWS § 9-34-8 (1992); S.C. CODE ANN. 16-17-710 (2006); WIS. STAT. § 42.07 (1990); VA. CODE ANN. § 15.2-969 (2009).

and wire fraud laws to accomplish something Congress and New Jersey have decided not to do. This is neither proper nor wise.

III. IMPOSING CRIMINAL LIABILITY BASED ON TERMS OF SERVICE WOULD BE AN EXTRAORDINARY AND DANGEROUS EXTENSION OF CRIMINAL LAW

Basing criminal liability on whether a person has fully complied with terms of service is extraordinarily dangerous. Criminal punishment cannot be based on the vagaries of privately created, frequently unread, generally lengthy and impenetrable terms of service implemented to further the business interests of e-commerce sites, and not necessarily the public interest.

A. Website Policies, Including Those Of The OTVs, Contain Items That Are Likely Routinely Violated, Thus Making Potentially Millions Of Americans Into Criminals Under the Government's Theory

Website terms of service often include capricious provisions that are violated millions of times every day by Internet users. According to the Government's argument, these users violate federal law every time they breach the terms of service unilaterally imposed by websites, regardless of how unreasonable those terms may be.

For example, Ticketmaster's terms provide:

- You will not use Ticketmaster if you are under 13 without parental consent.²⁵
- You will not "record or transmit, or aid in recording or transmitting, any description, account, picture, or reproduction" of events for which you buy tickets.²⁶
- You consent to searches of your person and belongings upon entry to events.²⁷
- You grant Ticketmaster and event providers permission to "utilize your

²⁵ Ticketmaster Terms of Use, <http://www.ticketmaster.com/h/terms.html> (last visited June 25, 2010).

²⁶ Ticketmaster Purchase Policy, <http://www.ticketmaster.com/h/purchase.html> (last visited June 25, 2010).

²⁷ *Id.*

name, image, likeness, acts, poses, plays, appearance, movements, and statements in any live or recorded audio, video, or photographic display or other transmission, exhibition, publication or reproduction” made of, or at the event[.]”²⁸

Under the government’s theory, a twelve-year-old user becomes a criminal when she buys a ticket from Ticketmaster without explicit parental permission. And if a Ticketmaster user takes notes at a concert for purposes of writing a review for a newspaper, or refuses to be patted down when entering an event, or objects to being photographed by representatives of Ticketmaster or the event organizer during an event, she commits a computer crime.²⁹

This is not an isolated problem; Ticketmaster is not the only OTV to impose arbitrary terms of service upon users. Tickets.com, for example, seeks to prohibit individuals from accessing its site with the intent to purchase tickets for resale, regardless of whether they use automated means or purchase in bulk. *See* Tickets.com Terms of Use, http://www.tickets.com/aboutus/user_agreement.html (last visited June 30, 2010) (“If you are seeking to purchase tickets to any event offered through this website for the purposes of reselling those tickets, then you are not authorized to enter this website and use its services.”); *see also* Telecharge.com Policies, <http://www.telecharge.com/policies.aspx> (last visited June 30, 2010) (“You may not copy, modify, distribute, display, perform, create derivative works from, transfer or sell any information, software, products or services obtained from this web site.”). Purchasing

²⁸ *Id.*

²⁹ It is of no import that law enforcement might not choose to bring these cases. The inability of a reader to distinguish in a meaningful and principled way between innocent and criminal computer usage is the constitutional harm. *Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998). *See also* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, Minn. L. Rev. (forthcoming 2010) at 17, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187 (“Courts must adopt a meaning of unauthorized access that does not let the police arrest whoever they like. This means that courts must reject interpretations of unauthorized access that criminalize routine Internet use or that punish common use of computers.”).

a ticket on Tickets.com with the intent to resell it is simply outside the purview of federal criminal law.

Nor would such an expansive reading of the CFAA or the dangerous impact of creating criminal liability for violations of terms of use be limited to ticket websites. Google bars use of its services by minors – probably to protect itself against liability and to try to ensure its terms are binding in the event of a litigated dispute, but not because it intends for any minor who uses the Google search engine to be prosecuted.³⁰

In another example, YouTube's Community Guidelines, expressly incorporated into the site's terms of use, prohibit posting videos that show "bad stuff." YouTube Community Guidelines, http://www.youtube.com/t/community_guidelines (last visited June 18, 2010). Uploading "bad stuff" would not only violate YouTube's terms of service, but under the government's theory here also constitute access without permission to the site. Surely YouTube did not draft the "bad stuff" prohibition with criminal liability in mind. Whatever the validity of holding such contracts enforceable for purposes of contract law,³¹ the terms cannot define the line between lawful conduct and criminal violations.

The popular social networking service Facebook has terms of service that are also probably routinely violated. For instance, Facebook's terms of use provide:

- You will not provide any false personal information on Facebook.
- You will keep your contact information accurate and up-to-date.

³⁰ Google Terms of Service § 2.3, <http://www.google.com/accounts/TOS> (last visited June 30, 2010) ("You may not use the Services and may not accept the Terms if (a) you are not of legal age to form a binding contract with Google, or (b) you are a person barred from receiving the Services under the laws of the United States or other countries including the country in which you are resident or from which you use the Services.").

³¹ See Mark A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459, 465, 475-76 (2006) (observing that in civil cases "in today's electronic environment, the requirement of assent has withered to the point where a majority of courts now reject any requirement that a party take any action at all demonstrating agreement to *or even awareness of terms* in order to be bound by those terms.") (emphasis added). This lax approach simply cannot provide "fair notice" in the criminal context.

- You will not share your password . . . [or] let anyone else access your account[.]³²

Under the government's theory in this case, if a user shaves a few years off of her age in her profile information, or asserts that she is single when she is in fact married, or seeks to obfuscate her current physical location, hometown or educational history for any number of legitimate reasons, she violates federal computer crime law. And if a user changes jobs or moves to another city, she must immediately inform Facebook or run the risk that her continued use of the site could lead to criminal sanctions. Moreover, a politician or other high-profile user who communicates through Facebook with the general public violates the terms of service if he delegates his password to employees or volunteers to maintain his page. *See, e.g.,* Barack Obama's Facebook Page, <http://www.facebook.com/barackobama> (last visited June 20, 2010) (prominently noting that the page is "run by Organizing for America, the grassroots organization for President Obama's agenda for change.").

These activities may breach a website's terms of service, but it defies logic that such conduct should be criminally punishable. The Court should reject the government's theory that terms of service violations are computer crimes.

B. Web Site Terms Are Created by Private Site Owners for a Myriad of Business Reasons Having Nothing To Do With The Public Interest or With Regulating "Access" for CFAA Purposes

Punishing terms of service violations is particularly concerning because terms written by private parties are typically intended to protect their own business interests, not benefit society at large. Website owners and Internet businesses draft specific terms of use provisions for a variety of reasons that have nothing to do with regulating "access" to their sites, and certainly nothing to do with preventing the sort of unauthorized hacking or trespass or theft of private data with which the CFAA is properly concerned. *See*

³² Facebook Statement of Rights and Responsibilities § 2, <http://www.facebook.com/terms.php> (last visited June 20, 2010).

United States v. Drew, 259 F.R.D. 449, 465 (C.D. Cal. 2009) (“utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime improperly makes the website owner the party who ultimately defines the criminal conduct”). Google, for example, presumably included the terms of use provision described earlier – barring use of its services by minors – to protect itself against liability and to try to ensure its terms were binding in the event of a litigated dispute. Surely it did not mean – or imagine – that tens of millions of minors in fact would never use its services to obtain information or would do so at the risk of criminal liability.

Enforcing contractual terms with the club of criminal law will have anti-competitive consequences, hinder innovation and thwart user choice. The Court should be especially careful not to suggest that criminal liability attaches when a user or user-directed service violates a term or condition that seeks to hamper competing services, as may be the case here.

For example, as described above, Ticketmaster, a named victim in this case, owns TicketsNow.com, a secondary ticket marketer. TicketsNow gets its inventory from primary sources that choose to sell some tickets at higher than face value. In contrast, Defendants supply tickets via brokers to competitors of Ticketmaster and TicketsNow. So the fewer tickets Defendants can buy, the fewer tickets are available from competitors, and the greater advantage TicketsNow has in the secondary market. Criminal enforcement of Ticketmaster’s terms of service thus chills effective competition in the supply of tickets to the secondary market, effectively “stacking the deck” for Ticketmaster and its subsidiary and creating severe punishments for competitors. The government’s urged interpretation of the CFAA runs the very serious risk of allowing Ticketmaster to limit competitors to utilizing only the innovation that Ticketmaster chooses to allow through its terms of service. If the Court allows enforcement of terms of service through criminal law, consumer choice could very well be limited not by natural

competition, but a company's privately imposed – but publicly enforced – terms, the penalty for non-compliance with which would be unacceptably steep.

C. Terms of Service are Often Poorly Accessible, Hard to Understand and Rarely Read.

Like the OTVs' websites here, many web-based services post their terms behind a "legal notices" or "terms of service" hyperlink that users can only access by scrolling to the bottom of the page and clicking on the link. Nothing about the links indicate that they are exceptionally important, much less that failure to click on them and read the underlying terms could subject the user to criminal penalties. The fallacy of any notion that Internet users are on "fair notice" that disregarding the terms of service of the many web sites and web services they visit puts them at risk of serious criminal liability is revealed by the widespread (and widely accepted) understanding that large numbers of users never read these terms, or read and understand only limited portions of them.

For example, to access the Ticketmaster terms of use, one must scroll down to find a hyperlink labeled "terms." Merely by visiting the website, the user agrees to be bound by Ticketmaster's Terms of Use, Privacy Policy, Purchase Policy, TicketExchange Selling Policy, Ticketmaster Auction Terms,³³ and "any other policies, rules or guidelines that may be applicable to particular offers or features on the Site".³⁴ In other words, a user is bound by multiple agreements that she likely has never read, and which may or may not be supplemented by other unspecified "policies, rules or guidelines" at Ticketmaster's option.

Furthermore, many websites and other online services present terms of service that are lengthy and impenetrable. In one particularly daunting example, Network Solutions, the domain name registrar, has a terms of service that takes up 128 pages when pasted into a single spaced, 12-point font Microsoft Word document. *See* Network

³³ When cut and pasted end to end into a Microsoft Word document, these five policies are collectively 29 pages long.

³⁴ Ticketmaster Terms of Use, *supra* at note 25.

Solutions Terms of Service, <http://www.networksolutions.com/legal/static-service-agreement.jsp> (last visited June 29, 2010). Not surprisingly, many commentators recognize that few consumers actually take the time to read and understand digital terms of service (or similar software download agreements) before saying they agree to them. *See* Restatement (Second) of Contracts § 211, cmt. b (1981) (“Customers do not . . . ordinarily understand or even read the standard terms.”); Robert L. Oakley, *Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts*, 42 Hous. L. Rev. 1041, 1051 (2005) (“Clickwrap licenses are ubiquitous today, and most people click to accept without reading the text.”); Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. Rev. 429, 429-31 (2002) (“with increasing alacrity, people agree to terms [in clickwrap contracts] by clicking away at electronic standard forms on web sites and while installing software”); Michael I. Meyerson, *The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts*, 47 U. Miami L. Rev. 1263, 1269 & nn. 28-29 (1993), (citing cases recognizing the failure of most consumers to read form contracts).

In one notable experiment, a software company surreptitiously inserted into its license agreement an offer to pay \$1000 to the first person to send an email to a particular address. It took four months and more than 3000 installations before someone noticed the offer and claimed the prize. Jeff Gelles, *Internet Privacy Issues Extend to Adware*, Newark Star-Ledger, July 31, 2005, at 5. *See also* *Ting v. AT&T*, 182 F. Supp. 2d 902, 930 (N.D. Cal. 2002), (holding a customer service agreement procedurally unconscionable because lack of notice contributed to surprise, the court acknowledged that “AT&T’s own research found that only 30% of its customers would actually read the entire CSA [consumer service agreement] and 10% of its customers would not read it at all”).

Empirical research confirms that, in the online context, a majority of users

ignored the terms of use entirely when installing such popular software as Google Toolbar on their home computers. Nathaniel Good et al., Commentary, *User Choices and Regret: Understanding Users' Decision Process About Consensually Acquired Spyware*, 2 I/S: J.L. & Pol'y for Info. Soc'y 283, 321 (2006). Moreover, even the few people who do read the terms of service are unlikely to take notice of more than a handful of the provisions. Due to human cognitive limitations, even rational consumers will be ignorant of non-salient terms in form contracts. Melvin Aron Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 Stan. L. Rev. 211, 244 (1995).

To make matters worse, most website terms, like other form contracts, are written in impenetrable legalese and poorly organized. See Robert W. Gomulkiewicz, *Getting Serious About User-Friendly Mass Market Licensing for Software*, 12 Geo. Mason L. Rev. 687, 692-94, 701-02 (2004). Such contracts often written at a level of difficulty that exceeds the ability of most consumers to understand. See Alan M. White & Cathy Lesser Mansfield, *Literacy and Contract*, 13 Stan. L. Rev. 233, 235-42 (2002). Drafters of these agreements give little attention to readability, instead relying heavily on legal boilerplate and including restrictive terms primarily designed to limit the company's exposure to liability. See Gomulkiewicz, *supra*, at 692-94, 701-02; Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. Chi. L. Rev. 1203 (2003). Given the difficulty of comprehending form contracts, and the typically low-dollar amount of the transactions to which they apply, a consumers' decision to forego reading a website's terms of use is not only common, but also entirely rational. Eisenberg, *supra*, at 240-44; Meyerson, *supra*, at 1269-70. Thus, even persons who are conscientious about reading the terms of service may be unaware of some of the provisions. Under these circumstances, whatever the validity of holding such contracts enforceable for purposes of contract law, the transformation of their terms into the defining criteria for serious criminal violations creates serious risks of criminal sanctions

for unwitting violations that cannot pass vagueness and notice review.

This problem is exacerbated by the fact that many terms of service contain clauses which state that the website owner can unilaterally change the terms, and that continued use of the website implies acceptance of whatever new terms have been added. For example, Ticketmaster's terms of service states that the company can change the terms at any time, and that continued use of the website constitutes automatic acceptance of any new terms.³⁵ Under the government's expansive view of the CFAA, a person's access to Ticketmaster would be unauthorized or would exceed their authorization if that person used the service and inadvertently violated a newly added or updated provision of the terms that had been inserted since the last visit. However challenging such a view of notice to a contract's terms may be for civil contract law, it fundamentally cannot be said to constitute adequate "fair notice" for due process vagueness purposes. *See Douglas v. U.S. Dist. Court for Cent. Dist. Calif.*, 495 F.3d 1062, 1066 & n.1 (9th Cir. 2007) (holding that website users are not required to continually monitor a site's terms of use for possible changes).

IV. APPLICATION OF THE CFAA WHEN A USER IGNORES OR VIOLATES WEBSITE TERMS OF SERVICE WOULD VIOLATE DUE PROCESS AND RENDER THE STATUTE VOID FOR VAGUENESS

Grounding criminal liability under section 1030(a)(2)(C) on whether a person has complied with the vagaries of privately created, frequently unread, generally lengthy and impenetrable terms of service would strip the statute of adequate notice to citizens of what conduct is criminally prohibited and render it hopelessly and unconstitutionally

³⁵ Ticketmaster Terms of Use, *supra*, note 25; *see, e.g.*, West Terms of Use, <http://west.thomson.com/about/terms-of-use/default.aspx?promcode=571404> (last visited June 21, 2010) ("By accessing, browsing, or using this website, you acknowledge that you have read, understood, and agree to be bound by these Terms. We may update these Terms at any time, without notice to you. Each time you access this website, you agree to be bound by the Terms then in effect."); AOL Terms of Use, http://about.aol.com/aolnetwork/aolcom_terms (last visited June 21, 2010) ("You are responsible for checking these terms periodically for changes. If you continue to use AOL.COM after we post changes to these Terms of Use, you are signifying your acceptance of the new terms.").

vague. The Supreme Court has stated:

“[i]t is a fundamental tenet of due process that ‘[n]o one may be required at peril of life, liberty or property to speculate as to the meaning of penal statutes.’ *Lanzetta v. New Jersey*, 306 U.S. 451, 453 (1993). A criminal statute is therefore invalid if it ‘fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden’ *United States v. Harriss*, 347 U.S. 612 (1954).”

United States v. Batchelder, 442 U.S. 114, 123 (1979); *see also Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972).

A plurality of the Supreme Court has further specified that “[v]agueness may invalidate a criminal law for either of two independent reasons. First, it may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement.” *Chicago v. Morales*, 527 U.S. 41, 56 (1999) (Stevens, J., plurality opinion).

In the Third Circuit, to survive vagueness review, a statute must (1) define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and (2) endow avoiding officials with undue discretion to determine whether a given activity contravenes the law’s mandates. *See Kreimer v. Bureau of Police for Town of Morristown*, 958 F.2d 1242, 1266 (3d Cir. 1992) (“[A] vagueness challenge will succeed when a party does not have actual notice of what activity the statute prohibits. Yet the vagueness doctrine, unlike the overbreadth doctrine, additionally seeks to ensure fair and non-discriminatory application of the laws, thus reflecting its roots in the due process clause. Accordingly, it finds repulsive laws that endow officials with undue discretion to determine whether a given activity contravenes the law’s mandates.” (citations omitted)).

For these reasons, George Washington Law Professor Orin Kerr has argued thoughtfully and persuasively that “unauthorized access” should not include access to a computer in violation of a contract or terms of service. Professor Kerr observes that

doing so would:

threaten a dramatic and potentially unconstitutional expansion of criminal liability in cyberspace. Because Internet users routinely ignore the legalese that they encounter in contracts governing the use of websites, Internet Service Providers (ISPs), and other computers, broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web.

Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1599 (2003). Consider the remarkable and disturbing results that a contract-based approach to criminalizing computer access can create:

Imagine that a website owner announces that only right-handed people can view his website, or perhaps only friendly people. Under the contract-based approach, a visit to the site by a left-handed or surly person is an unauthorized access that may trigger state and federal criminal laws. A computer owner could set up a public web page, announce that "no one is allowed to visit my web page," and then refer for prosecution anyone who clicks on the site out of curiosity. By granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner.

Id. at 1650-51.

The CFAA offers no guidance on the meaning of access or use "with permission." As Kerr argues, "The core difficulty is that access and authorization have a wide range of possible meanings. . . . Is it unauthorized if the computer owner tells the person not to access the computer? Is it unauthorized if the access is against the interests of the computer owner? Is it unauthorized if the access violates a contract on access? Presently the answer is remarkably unclear." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, Minn. L. Rev. (forthcoming 2010) at 17, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187.

Under the government's interpretation of section 1030, the statute must rely for its essential meaning on the existence and clarity of separate contractual terms drafted for a variety of reasons that have nothing to do with preventing the sort of unauthorized

hacking, misuse, trespass or theft of private data with which the computer crime law is properly concerned. Given that courts must adopt a narrow construction of a criminal statute to avoid vagueness, overbreadth and other unconstitutional infirmities, the government's proposed view of section 1030 must be rejected. *See Zadvydas v. Davis*, 533 U.S. 678, 689 (2001); *Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971) (law disallowing three people to congregate if it is annoying to others was unconstitutionally vague).

Choosing, as the government has here, to prosecute under the CFAA a single, isolated instance of violating terms or service out of literally millions of similar, ongoing violations illustrates the dangers of arbitrary enforcement. In a world where each violation or neglect of a website's terms could constitute unauthorized or excessive access and be the basis for criminal prosecution, there simply is no limiting principle that would restrain the exercise of this enforcement discretion and prevent arbitrary or discriminatory application of the law.

VII. CONCLUSION

For the foregoing reasons, the indictment should be dismissed.

DATED: July 2, 2010

ELECTRONIC FRONTIER FOUNDATION

By /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (California Bar No. 168423)

454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x134
Facsimile: (415) 436-9993